SCHÉMA DE SIGNATURE D'ANNEAU BASÉE SUR LES RÉSEAUX EUCLIDIENS

Carlos Aguilar-Melchor[*], **Slim Bettaieb**[*], **Laurent Fousse**[**], and **Philippe Gaborit**[*]

[(*)]XLIM-DMI, Université de Limoges, 123, av. Albert Thomas 87060 Limoges Cedex, France
[(**)]Google Inc, 1600 Amphitheatre Parkway Mountain View CA 94043, États Unis

Résumé

Aujourd'hui, il existe deux familles de signature numérique basée sur les réseaux euclidiens: une basée sur le principe hacher-et-signer de Gentry et al.; et les schémas de Lyubashevsky qui sont de type Fiat-Shamir.
Dans ce papier, on montre comment transformer le schéma de signature numérique proposé par Lyubashevsky [8] en un schéma de signature d'anneau. Notre schéma assure l'anonymat et l'inforgeabilité dans le modèle de l'oracle aléatoire.

Mots clés: Signature d'anneau, réseaux euclidiens.

1 INTRODUCTION

En 2001 Rivest, Shamir et Tauman ont intoduit le concepte de signature d'anneau. Dans un schéma de signature d'anneau, chaque utilisateur possède une paire de clés. Une clé de pour signer (secrète) et une clé publique de vérification. Pour générer une signature, le signataire peut choisir un sous ensemble de l'ensemble de toutes les clés publiques (dit anneau) qui contient sa propre clé publique puis il signe au nom de l'anneau sans la permission ou bien l'aide des autres utilisateurs. La signature peut être vérifiée en utilisant les clés publiques associés à l'anneau mais, il n'est pas possible d'identifier le signataire parmis les membres de l'anneau.

La plupart des schémas de signature d'anneau qui existent dans la littérature sont basés sur des problèmes difficiles de la théorie des nombres comme par exemple : la factorisation des grands nombres [1], le problème du logarithme discret [2, 3] et le problème de pairing bilinaire [4, 5]. Dans [6], Brakerski et Kalai proposent un schéma basé sur les réseaux où ils utilisent des approches de type hacher-et-signer et bonsai-tree. En utilisant la même approche Wang et Bo Sun [7] proposent deux autres schémas de signature d'anneau.

Le schéma de signature d'anneau basée sur les réseaux qui est l'objet de cet article est le premier qui est dérivé des schémas de type Fiat-Shamir proposés par Lyubashevsky. Ce schéma est instancié avec les mêmes paramètres que celui de la signature numérique de Lyubashevsky. On obtient ainsi des signatures d'anneaux de taille plus petite que celles de Brakerski et Kalai et de Wang et Bo. La taille des clés utiliées est, elle aussi, plus petite que celle proposé par les schémas dans [6, 7].

2 RÉSEAUX

Les réseaux euclidiens (voir Définition 1) ont suscités beaucoup de travaux à partir du 19^{eme} sciècle. Gauss commence à s'y intérésser en 1801, puis c'est au tour de Hermite en 1850 et Minkowski en 1896. De nos jours, ils peuvent être utilisés en cryptologie sous forme de cryptanalyse ou cryptographie. La cryptanalyse utilisant les réseaux est principalement lié à l'algorithme LLL proposé par Lenstra, Lenstra et Lovàz en 1982. Les problèmes difficiles présentés par Ajtai sur les réseaux en 1996 ont permis de construire des cryptosystèmes dont la sécurité dépond de ceux-ci. Les avantages de la cryptographie basée sur les réseaux par rapport à celle utilisée traditionellement et basée sur la théorie des nombres se résument en : la résistance contre les ordinateurs quantiques et de bonnes performances dû à la simplicité des opérations.

Définition 1 *Soit $B = \{b_1, \ldots, b_n\} \in \mathbb{Z}^n$ un ensemble de n vecteurs linéairement indépendants. Un réseau $\mathcal{L}$ de dimension n généré par B est défini par $\mathcal{L}(B) = \{Bc \mid c \in \mathbb{Z}^n\}$. B est la base du réseau $\mathcal{L}$.*

Dans [8] Lyubashevsky et Micciancio ont introduit une famille de fonctions de hachage $\mathcal{H}$. Les auteurs ont montré l'existence d'une réduction pire-cas/cas-moyen entre le fait de trouver des collisions sur ces fonctions de hachage et la résolution de problèmes standards des réseaux. Dans la suite, on notera les fonctions de hachage qui appartiennent à $\mathcal{H}$ par h, les vecteurs par des lettres $(a, b, \ldots)$ et les vecteurs de vecteurs par une lettre avec un chapeau $(\hat{a}, \hat{b}, \ldots)$.

3 SIGNATURE D'ANNEAU

Dans cette section, nous commençons par rappeler le schéma de signature numérique proposé dans [8]. Ensuite nous donnons une façon de le transformer en un schéma de signature d'anneau. Dans [8], le signataire a $\hat{s}$ comme clé (secrète) de signature et (h, S) comme clé (publique) de vérification, tel que $h(\hat{s}) = S$. Pour signer un message μ, le signataire prouve qu'il peut:

- Choisir un vecteur de vecteurs $\hat{y}$ (il le garde secret).
- Retourner un vecteur de vecteurs dont la différence de $\hat{y}$ est $\hat{s} \cdot e$, où e est un petit vecteur qui n'est pas de son choix.

Pour ce faire, le signataire choisit aléatoirement $\hat{y}$, il calcule $e = H(h(\hat{y}), \mu)$ (H une fonction de hachage cryptographique) et il retourne $(\hat{z}, e)$ comme signature avec $\hat{z} = \hat{s}e + \hat{y}$. Le vérifieur teste si $e = H(h(\hat{z}) - Se, \mu)$. Cela est vrai pour une le signature valide grâce à la linéarité de h, puisque $h(\hat{z}) - Se = h(\hat{s}e + \hat{y}) - Se = h(\hat{y}) + Se - Se = h(\hat{y})$.

Pour obtenir une signature d'anneau à partir de ce schéma, nous faisons deux modifications majeures. La première est d'assurer que chaque utilisateur a une clé publique une fonction $h_i \in \mathcal{H}$ qui satisfait $h_i(\hat{s}_i) = S$ où $\hat{s}_i$ est la clé secrète et S est fixé et partagé par tous les membres de l'anneau. La deuxième modification est de garder le signataire anonyme quand il signe un message. Nous le faisons, en ajoutant $\ell - 1$ variables aléatoires qui correspondent aux membres de l'anneau sauf le vrai signataire. Par exemple, supposons que le vrai signataire est indexé par $j \in [\ell]$, le signataire envoi $(\hat{z}_i; i \in [\ell], e)$ comme signature avec $e = H(\sum_{i \in [\ell]} h_i(\hat{y}_i), \mu)$, $\hat{z}_j = \hat{s}_j e + \hat{y}_j$ et pour tout $i \in [\ell] \setminus \{j\}$, $\hat{z}_i = \hat{y}_i$ où $\hat{y}_i$ est choisi aléatoirement à partir d'une distribution uniforme. Par conséquent la signature contiendra ℓ éléments où chacun correspond à un memebre de l'anneau. Maintenant nous revenons à la première modification et nous allons démontrer son utilité. Pour la vérification de la signature, le vérifieur teste si le haché de $(\sum_{i \in [\ell]} h_i(\hat{z}_i) - Se, \mu)$ est égal à e. Noter que ce sera vrai seulement si $\sum_{i \in [\ell]} h_i(\hat{z}_i) - Se$ est égale à $\sum_{i \in [\ell]} h_i(\hat{y}_i)$. En effet, grâce à la linéarité de h_j nous avons $h_j(\hat{z}_j) = h_j(\hat{s}_j e + \hat{y}_j) = h_j(\hat{y}_j) + Se$. Puisque tous les membres de l'anneau ont des paires de clés $(h_i, \hat{s}_i)$ tel que $h_i(\hat{s}_i) = S$, le vérifieur pourra toujours accepter la signature quand l'un d'eux l'aura produite.

Le théorème suivant résume les propriétés de sécurité que notre schéma de signature d'anneau vérifie.

Théorème 1 *Le schéma de signature d'anneau qu'on propose est :*

- *Anonyme contre les attaques de type exposition complète de clé.*
- *Infalsifiable dans le cadre d'une corruption interne.*

Si le problème de plus court vecteur d'un réseau est difficile.

La preuve de ce théorème est la contribution principale de notre article. On montre qu'un attaquant qui est capable de forger une signature sera capable aussi de trouver des collisions sur les fonctions de hachages $h \in \mathcal{H}$. D'après la réduction pire-cas/cas-moyen dans [8], on obtient un algorithme qui peut résoudre le problème de plus court vecteur d'un réseaux SVP avec une approximation polynomial en paramètre de sécurité.

References

[1] How to leak a secret. Advances in Cryptology-ASIACRYPT 2001, pages 552–565, 2001.

[2] 1-out-of-n signatures from a variety of keys. Advances in Cryptology-Asiacrypt 2002, pages 639–645, 2002.

[3] Forking lemmas for ring signature schemes. Progress in Cryptology-INDOCRYPT 2003, pages 266–279, 2003.

[4] An efficient signature scheme from bilinear pairings and its applications. Public Key Cryptography–PKC 2004, pages 277–290, 2004.

[5] Efficient ring signatures without random oracles. Public Key Cryptography–PKC 2007, pages 166–180, 2007.

[6] A framework for efficient signatures, ring signatures and identity based encryption in the standard model. Technical report, Cryptology ePrint Archive, Report 2010086, 2010.

[7] Ring signature schemes from lattice basis delegation. Information and Communications Security, pages 15–28, 2011.

[8] Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In Advances in Cryptology - ASIACRYPT 2009, pages 598–616, 2009.